Aegentra
ACADEMY

Enterprise Risk Register — AS ISO 31000:2018

Worked example — an ASX-listed Australian services business with a regulated subsidiary

Scored with the calibrated scales published alongside this file. Note the "within appetite?" and "control effectiveness" columns: a register that records only scores cannot tell a board whether anything needs to change. Twelve risks across strategic, operational, compliance, people, financial, technology, supply chain, safety, reputation and governance.

RISK ID	CATEGORY	RISK DESCRIPTION (EVENT - CAUSE - EFFECT)	CONSEQUENCE TYPE	INHERENT LIKELIHOOD	INHERENT CONSEQUENCE	INHERENT SCORE	INHERENT RATING	CURRENT CONTROLS	CONTROL EFFECTIVENESS	RESIDUAL LIKELIHOOD	RESIDUAL CONSEQUENCE	RESIDUAL SCORE	RESIDUAL RATING	WITHIN APPETITE?	TREATMENT DECISION	FURTHER ACTION	RISK OWNER	REVIEW FREQUENCY
ERM-001	Strategic	Loss of the largest client (28% of revenue) at contract renewal because the relationship sits with a single account director	**Financial**	3	5	15	High	Executive sponsor assigned; multi-year contract with 12-month notice; quarterly business reviews	Partially effective	2	5	10	High	No	Treat	Reduce single-client concentration below 20% of revenue over 24 months; add a second named relationship owner	Chief Executive	Quarterly
ERM-002	Operational	Failure of the core scheduling platform during peak period disrupts service delivery to all clients	Service delivery	3	4	12	High	Vendor SLA with 99.9% availability; documented manual fallback; nightly backups	Partially effective	2	4	8	Medium	Yes	Treat	Test the manual fallback under load; add a contractual right to audit the vendor	Chief Operating Officer	Quarterly
ERM-003	Compliance	Regulated subsidiary breaches licence conditions because obligations are tracked in a spreadsheet with no owner	**Regulatory and legal**	3	5	15	High	Annual compliance attestation; external legal review at renewal	Ineffective	2	4	8	Medium	No	Treat	Implement an obligations register with named accountable owners and automated review dates	Chief Risk Officer	Monthly
ERM-004	People	Sustained inability to recruit and retain qualified practitioners constrains delivery capacity and drives overtime fatigue	People and safety	4	3	12	High	Market-benchmarked remuneration; graduate pipeline; flexible working	Partially effective	3	3	9	Medium	Yes	Treat	Introduce a workforce plan with 12-month capacity forecasting; monitor overtime as a leading indicator	Chief People Officer	Quarterly

RISK ID	CATEGORY	RISK DESCRIPTION (EVENT - CAUSE - EFFECT)	CONSEQUENCE TYPE	INHERENT LIKELIHOOD	INHERENT CONSEQUENCE	INHERENT SCORE	INHERENT RATING	CURRENT CONTROLS	CONTROL EFFECTIVENESS	RESIDUAL LIKELIHOOD	RESIDUAL CONSEQUENCE	RESIDUAL SCORE	RESIDUAL RATING	WITHIN APPETITE?	TREATMENT DECISION	FURTHER ACTION	RISK OWNER	REVIEW FREQUENCY
ERM-005	Financial	Cash flow pressure from extended debtor days at two major clients breaches a banking covenant	Financial	2	5	10	High	Monthly cash flow forecasting; covenant headroom monitored; invoice finance facility available	Effective	1	5	5	Medium	Yes	Tolerate	Monitor; escalate if headroom falls below 15%	Chief Financial Officer	Monthly
ERM-006	Technology	Ransomware encrypts corporate file shares and backups because backup isolation was never verified	**Service delivery**	3	5	15	High	Immutable offsite backups; EDR on all endpoints; phishing-resistant MFA; annual restore test	Partially effective	2	4	8	Medium	No	Treat	Verify backup immutability by attempting deletion from a compromised admin account during the next test	Chief Technology Officer	Quarterly
ERM-007	Supply chain	A critical single-source subcontractor enters administration mid-contract	Service delivery	2	4	8	Medium	Annual financial health check; contractual step-in rights	Partially effective	2	3	6	Medium	Yes	Treat	Qualify a second supplier for the two highest-volume service lines	Chief Operating Officer	Half-yearly
ERM-008	Safety	Field staff sustain a serious injury during client site work because site inductions vary by client	**People and safety**	3	4	12	High	WHS management system; incident reporting; annual training	Partially effective	2	4	8	Medium	No	Treat	Standardise a pre-work hazard assessment independent of the client induction	General Manager Operations	Monthly
ERM-009	Reputation	A data breach affecting client personal information triggers Notifiable Data Breach reporting and national coverage	Reputation	2	5	10	High	Encryption at rest and in transit; access reviews; incident response plan tested annually	Effective	2	4	8	Medium	Yes	Treat	Rehearse the external communications limb of the incident response plan	Chief Risk Officer	Quarterly
ERM-010	Strategic	Failure to adapt the service model to AI-enabled competitors erodes margin over 3-5 years	Financial	3	4	12	High	Annual strategy review; innovation budget allocated	Partially effective	3	3	9	Medium	Yes	Treat	Commission a competitive position review; set a measurable margin-defence target	Chief Executive	Half-yearly

RISK ID	CATEGORY	RISK DESCRIPTION (EVENT - CAUSE - EFFECT)	CONSEQUENCE TYPE	INHERENT LIKELIHOOD	INHERENT CONSEQUENCE	INHERENT SCORE	INHERENT RATING	CURRENT CONTROLS	CONTROL EFFECTIVENESS	RESIDUAL LIKELIHOOD	RESIDUAL CONSEQUENCE	RESIDUAL SCORE	RESIDUAL RATING	WITHIN APPETITE?	TREATMENT DECISION	FURTHER ACTION	RISK OWNER	REVIEW FREQUENCY
ERM-011	Project	The finance system replacement overruns budget and delays statutory reporting	Financial	3	3	9	Medium	Stage-gated governance; independent quality assurance at each gate	Effective	2	3	6	Medium	Yes	Tolerate	Monitor at the project steering committee	Chief Financial Officer	Monthly
ERM-012	Governance	Board risk oversight is ineffective because reporting shows a heat map with no trend or appetite context	**Regulatory and legal**	4	3	12	High	Quarterly risk report to the Audit and Risk Committee	Ineffective	2	3	6	Medium	No	Treat	Replace the heat map with appetite-versus-actual trending and named KRIs with thresholds	Chief Risk Officer	Quarterly

Free to use and adapt. This template is published in full by Aegentra Academy, an official PECB authorised training partner in Australia. Get the rest of the set and the course it accompanies at aegentra.com.au/academy/iso-31000-risk-manager.